
# Semiannual Report to Congress

## April 1 – September 30, 2005

OIG

Office of Inspector General

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

October 31, 2005

The Honorable Alan Greenspan
Chairman
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Chairman Greenspan:

We are pleased to present our *Semiannual Report to Congress* which summarizes the activities of our office for the reporting period April 1, 2005, through September 30, 2005. The Inspector General Act requires that you transmit this report to the appropriate committees of Congress within thirty days of receipt, together with a separate management report and any comments you wish to make.

Sincerely,

*/signed/*

Barry R. Snyder
Inspector General

Enclosure


# Semiannual Report to Congress

## April 1 – September 30, 2005

OIG

Office of Inspector General

# Table of Contents

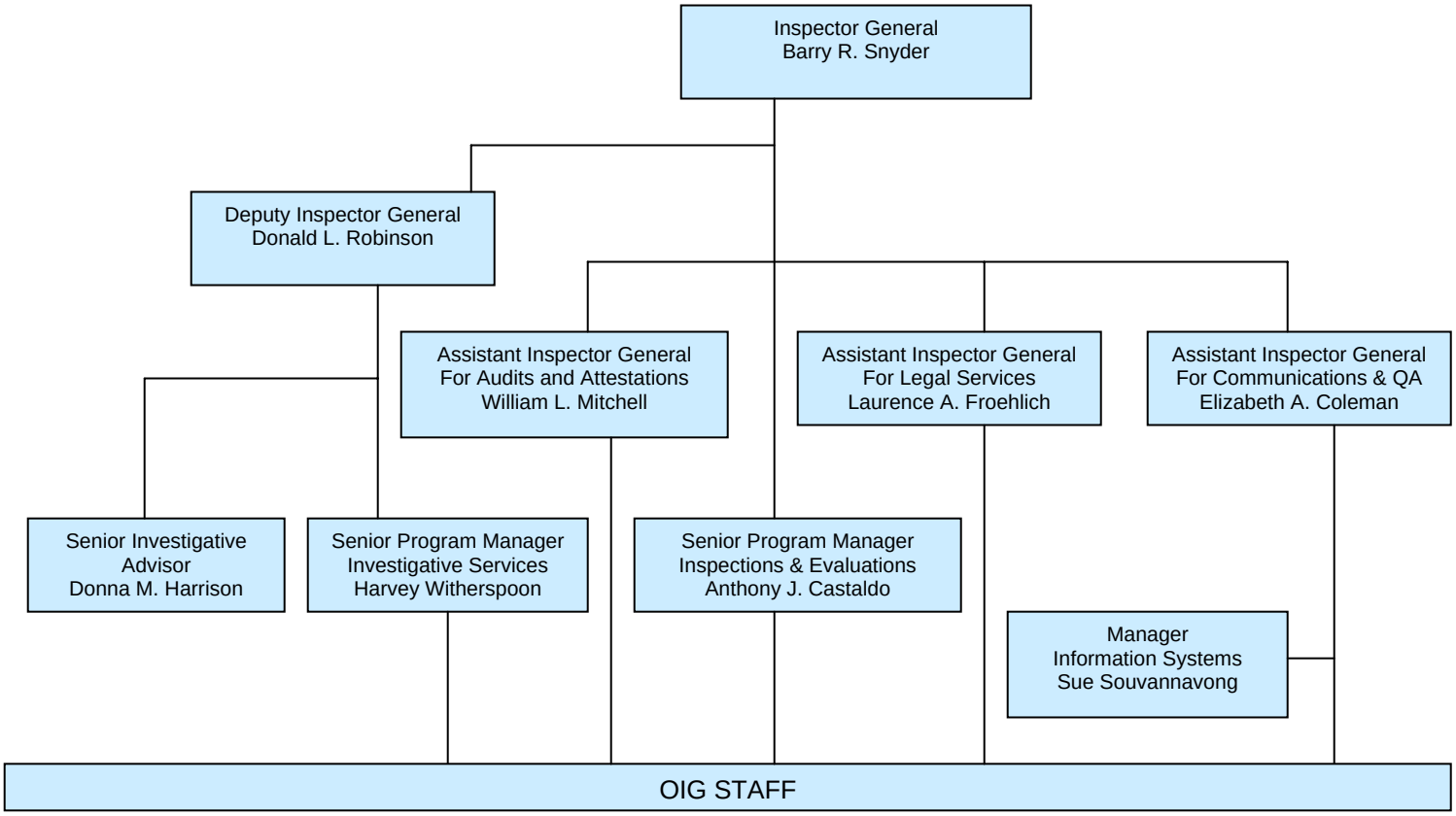
# Introduction

Consistent with the Inspector General Act of 1978 (IG Act), as amended, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- conduct and supervise independent and objective audits, investigations, and other reviews of Board programs and operations;
- promote economy, efficiency, and effectiveness within the Board;
- help prevent and detect fraud, waste, and mismanagement in the Board's programs and operations;
- review existing and proposed legislation and regulations and make recommendations regarding possible improvements to the Board's programs and operations; and
- keep the Chairman and Congress fully and currently informed of problems.

Congress has also mandated additional responsibilities that impact where the OIG directs its resources. For example, section 38(k) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. 1831o(k), requires the Board's OIG to review failed financial institutions supervised by the Board that result in a material loss to the bank insurance funds, and to produce, within six months of the loss, a report that includes possible suggestions for improvement in the Board's banking supervision practices. In the information technology arena, the Federal Information Security Management Act of 2002 (FISMA), Title III of Public Law 107-347, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Consistent with FISMA's requirements, we perform an annual independent evaluation of the Board's information security program and practices to include evaluating the effectiveness of security controls and techniques for selected information systems.

# OFFICE OF INSPECTOR GENERAL
# September 2005



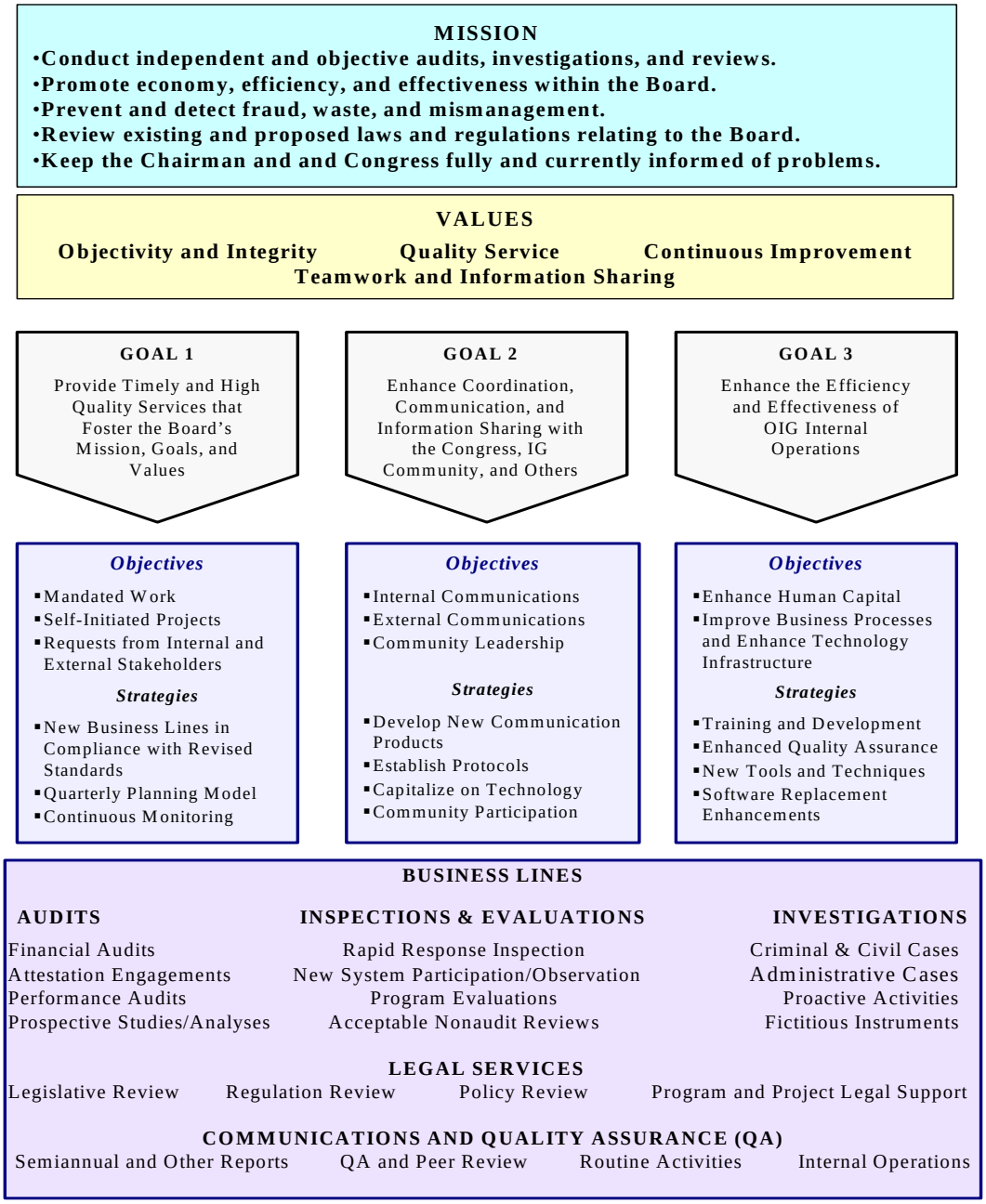

OIG Staffing

| | |
|---|---|
| **Auditors** | **15** |
| **EDP Auditors** | **5** |
| **Investigators** | **5** |
| **Attorneys** | **2** |
| **Administrative** | **1** |
| **Information Systems Analysts** | **3** |
| Total Positions | 31 |

# Goals and Objectives

The OIG has identified three strategic goals and developed corresponding objectives to guide our work through 2008. For each strategic goal, we have also identified specific strategies to help achieve the underlying objectives. The exhibit below depicts the relationship of the various elements of our strategic plan, within the context of our mission and values.

## Overview of the OIG's Strategic Plan, 2005- 2008



# Projects Completed during this Reporting Period

### *Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act*

The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA requires agencies to provide information security protections for (i) information collected or maintained by or on behalf of the agency, and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Although the Federal Reserve Banks are not directly subject the legislation, the Banks perform functions under delegated authority from the Board. In performing these functions, the Reserve Banks collect or maintain information and use or operate information systems on behalf of the Board. This information and these information systems are therefore subject to FISMA's requirements.

We conducted this audit as part of our effort to perform work throughout the year related to our independent evaluation responsibilities under FISMA. Our objectives were to evaluate (1) the policies and procedures established by the Division of Banking Supervision and Regulation (BS&R) and the Division of Information Technology (IT) to ensure that applications owned or operated by Reserve Banks on behalf of the Board meet FISMA's requirements, and (2) the Reserve Bank's implementation of those policies and procedures, focusing specifically on how the application inventories were compiled.

Overall, we found that the Federal Reserve System (System) has begun implementing FISMA's requirements for Supervision and Regulation (S&R) systems. During 2004, BS&R established a project team to help the S&R business function at the Reserve Banks comply with the legislation. In addition to conducting FISMA awareness training at the Reserve Banks, the project team also issued guidance for developing an inventory of applications, developed an application tracking mechanism, and established a process to track identified weaknesses and associated corrective actions. Based on the guidance provided, the Reserve Banks developed an initial inventory of applications and completed several security control reviews using a self-assessment questionnaire.

Notwithstanding the progress made, however, we believe that further actions are required to ensure that information and information systems used or operated by the Reserve Banks in support of S&R delegated functions meet FISMA's requirements. We found that the Reserve Banks did not follow a consistent approach to developing their application inventory, and the guidance issued to the Reserve Banks for developing the inventory was insufficient to address all security controls and properly establish system interfaces as required by FISMA. We also found that guidance issued to the Reserve Banks did not thoroughly address other aspects of the Board's current information security program (such as developing security

plans, testing application security controls, and implementing corrective action plans).

Our report contains four recommendations designed to enhance guidance to the Reserve Banks, strengthen compliance with the legislation and the Board's security program, and establish greater consistency across the System. We provided our report to the Director of IT, who serves as the Board's CIO for FISMA, and to BS&R's Chief Technology Officer for review and comment. Their response partially concurred with our first recommendation, did not concur with our second recommendation, and generally concurred with the intent of our other recommendations. For all four recommendations, the response identified actions that, if fully implemented, will generally satisfy the recommendations' intent. Work on this audit also identified broader issues related to the Board's approach to, and progress towards, implementing portions of its information security program. These issues were addressed as part of our annual evaluation of the Board's information security program.

### *Audit of the Board's Information Security Program*

We performed this audit pursuant to FISMA's requirement that each agency Inspector General (IG) conduct an annual independent evaluation of the agency's information security program and practices. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate compliance by the Board with FISMA and related information security policies, procedures, standards, and guidelines.

To evaluate security controls and techniques, we reviewed controls over three applications running primarily on the Board's Unix and Linux platforms. Because this year's reporting guidance from the Office of Management and Budget (OMB) required IGs to include applications operated by contractors or other sources as part of their control testing, we also reviewed controls over one application maintained by the Federal Reserve Bank of Philadelphia in support of the Board's S&R function. Our security control tests did not identify any significant deficiencies, although we found areas where controls can be strengthened. We also reviewed configuration settings for selected devices such as servers, workstations, and routers maintained by Board staff. Our review of configuration settings found that the Board has enhanced the processes for establishing, monitoring, and remediating security settings, although we identified additional improvement opportunities. Given the sensitivity of the issues involved with our control testing and configuration reviews, we provided the specific results to management under separate restricted covers. In addition, we followed up on the status of the recommendations and observations made in prior control reviews and found that sufficient actions had been taken to close all open items.

To evaluate the Board's compliance with FISMA and related policies and procedures, we also followed up on the open recommendations from our 2004 information security audit report and reviewed the Board's processes related to certification and accreditation, remedial action monitoring, incident response, and security awareness and training. Because FISMA authorizes the IGs to base their annual evaluation in whole or in part on existing audits, evaluations, or reports relating to programs or practices of the agency, we also incorporated the results from our earlier audit of the System's efforts to implement FISMA requirements for applications operated by the Reserve Banks in support of the Board's delegated S&R function.

Our follow-up work showed that over the past year the Board has continued to make progress in developing and implementing a structured information security program as outlined by FISMA, and actions taken are sufficient to allow us to close two of our previous recommendations. Because other improvements related to our remaining recommendations are still in process, we left these recommendations open and will continue to review actions taken as part of our ongoing work related to information security. Notwithstanding this progress, however, we found that the Board has not yet identified all information and information systems supporting its operations and assets or fully implemented information security requirements for applications maintained by third parties. We also found that the Board's overall governance structure for information security has been ineffective in establishing, monitoring, and enforcing compliance with information security requirements. Our report contains two recommendations to address these issues.

In her response to our draft report, the Director of IT, in her capacity as the CIO for FISMA, stated that she shares our belief that the Board should identify all information collected and maintained and all information systems used or operated by the Board or on its behalf. The director also recognized that the appropriate authority and controls need to be in place to facilitate the effective implementation and continued compliance with FISMA. The director's response generally agreed with the intent of our recommendations and identified actions that the Board plans to implement as part of its information security activities. Specifically, the director's response stated that the Board plans to perform a more comprehensive review to identify all information and information systems used by the Board and determine whether or not that usage falls within FISMA's legislative requirements. Once that analysis is complete, the director indicated that the Board will reevaluate our recommendation regarding information security governance and make changes as appropriate in light of the final inventory and any additional developments from OMB. We will review these actions as part of our ongoing audit and evaluation work related to information security.

In addition to the two recommendations discussed above, our report also discussed continuing challenges for Board management related to information security. The Board's Information Security Officer (ISO) has developed a new

information security program and related processes based on National Institute of Standards and Technology (NIST) guidelines and standards, and has been working with divisions and offices over the past year to identify and categorize Board information and the related information systems as outlined in NIST's Federal Information Processing Standards 199. Additional phases of the ISO's revised program include updated security plans, risk assessments, and certifications and accreditations. The current implementation timeline projects that the revised program will be fully implemented for major applications by September 2006, and the ISO has projected that all non-major systems will be transitioned by 2007. We are concerned that the implementation timeline fails to meet OMB and NIST expectations and that it fails to include any Reserve Bank applications, even though these applications comprised about 50 percent of the Board's reported inventory as of August 2005. We discussed these concerns with the CIO and ISO during our closing meeting, and we will review the Board's progress towards implementing its revised program and processes as part of our ongoing work related to information security. During our audit, we also observed the Board's contingency testing activities and provided our observations in a separate briefing to Board senior management for their consideration.

### *Review of the Bank of Ephraim Failure*

During this period, we issued our *Report on the Failure of the Bank of Ephraim*. The Bank of Ephraim (BOE) was a small community bank with offices in central and southern Utah serving residents, businesses, and other institutions. As a state chartered member bank of the Federal Reserve System, BOE was supervised by the Federal Reserve Bank of San Francisco (FRB San Francisco) under delegated authority from the Board. The Commissioner of the Utah Department of Financial Institutions closed BOE on June 25, 2004, because losses attributed to an embezzlement by the institution's cashier rendered the bank insolvent. The FDIC estimated BOE's failure as a $4.7 million potential loss to the Bank Insurance Fund (BIF). We performed this review because the failure involved fraud and, in our view, the projected loss, totaling ten percent of the institution's assets, was relatively high. Our objectives were to ascertain why the institution's problems resulted in a loss to the BIF, and make recommendations, if warranted, for preventing any such loss in the future.

BOE failed because the institution's cashier exploited a weak corporate governance environment and inadequate internal control structure to embezzle funds and conceal the fraud by systematically manipulating the bank's financial records. Simultaneously, problems with the bank's loan portfolio were eroding available capital and, when the fraud was discovered, the bank was deemed undercapitalized and subsequently declared insolvent. We found that while Reports of Examination and examiner work papers consistently identified internal control weaknesses that often pointed to the cashier, FRB San Francisco did not compel bank management to take corrective action. In addition, FRB San

Francisco examination managers did not recognize the inherent risks posed by the recurrent nature of internal control deficiencies, and did not adjust the scope of subsequent examinations in accordance with risk-focused examination principles.

In our opinion, these longstanding and repeated weaknesses should have led to more in-depth testing which would have increased the likelihood that the fraud could have been uncovered earlier. We also found that FRB San Francisco examination managers did not fully recognize the cumulative magnitude of recurrent credit and loan administration weaknesses consistently identified by examiners. In our view, the timing, intensity, and scope of the informal supervisory actions taken were not commensurate with these risks. Accordingly, the bank continued its poor lending practices, which resulted in a high volume of inherently risky loans in the bank's southern Utah branch.

FRB San Francisco conducted a quality assurance review of BOE's supervision shortly after the bank was closed, and identified a number of factors that may have contributed to the Reserve Bank's failure to recognize the pattern of BOE's weaknesses. These factors included a lack of continuity in the management of BOE's supervision and significant staff turnover. FRB San Francisco has responded to the quality assurance review and other external assessments with a number of internal initiatives to strengthen examination planning, evaluations of internal controls, and the tools examination managers use to follow up on previous findings. We believe that these initiatives will help address many of the factors that contributed to lapses in BOE's supervision. We did not identify any deficiencies in the Federal Reserve's supervisory guidance and procedures; therefore, we are not making any formal recommendations.

The Director of BS&R reviewed our report, welcomed its contribution to understanding the failure of BOE, and highlighted the crucial importance of effective examination management and adherence to fundamental principles of risk-focused supervision. He noted that the division plans to monitor the progress of FRB San Francisco initiatives that respond to the issues raised by our report, and will ensure that copies are distributed to Reserve Bank senior officers, supervision management, and examiners. The director also said our report will be discussed with System supervision management groups and in examiner forums, and will be sent to the Staff Development Subcommittee of the Strategic Plan Steering Committee to determine if any changes or adjustments are warranted in the System's training programs.

### *Evaluation of Service Credit Computations*

Creditable service is a key component of the pension benefit calculation for Board employees. Creditable service includes current Board employment as well as prior service with the Federal Reserve System, the federal government, or the military. During this period, we performed an evaluation of service credit computations. Our

objectives were to verify the accuracy of recent service credit adjustments made by Management Division (MGT) staff, evaluate controls over the process of computing employees' creditable service, and evaluate the accuracy of service credit information in systems maintained by the Board and the outsourcing contractor.

Our recalculations showed that MGT staff accurately calculated the service credit adjustments for the employees in our sample. Management has also taken steps to strengthen the service credit process by training current staff and hiring additional knowledgeable staff to perform service credit calculations, implementing a supervisory review process, and developing an employee notification letter to inform employees of the types of prior service that are creditable and the steps they must take to receive credit. However, the process is manually-intensive and includes multiple data transcriptions which increases the risk of data errors. In addition, the process lacks several key controls; as a result, significant data discrepancies exist between the Board's information system and the system maintained by the outsourcing contractor. During our evaluation, we also identified other opportunities to strengthen existing controls.

We presented our evaluation results to the Deputy Director of MGT. Our briefing contained three recommendations designed to strengthen or enhance controls over the service credit process. Specifically, we recommended that MGT:

- strengthen controls by:
  - reducing or eliminating the number of data transcriptions,
  - requiring automated verifications from the outsourcing contractor for all data transmissions, and
  - performing periodic reconciliations between information systems.

- enhance existing controls by:
  - redesigning the prior creditable service form to provide additional space and clear instructions for documenting all applicable types of prior service, and
  - establishing a tickler file to ensure timely follow-up of pending files.

- provide periodic employee reminders regarding deposits/redeposits and renouncements (including dollar amounts) to help employees with retirement-related decisions.

The Deputy Director of MGT concurred with our recommendations and identified several actions that have been taken or are planned to address the recommendations. We will follow up on actions taken as part of future audit and evaluation work.

### *Review of the Board's Implementation of Software Security Reviews*

During this period, we completed a review of the processes used by the Board for requiring and performing software security reviews (SSRs). We began this

project as a result of questions raised during our 2004 annual audit of the Board's information security program. During that audit, we noted that the Board's information security program document incorporates procedures for performing SSRs based on requirements in its *Information Security Manual* (ISM). Specifically, SSRs are required on single purpose software that is used by business functions with a risk level of moderate or high. Because our audit identified at least one software package for which a review had not been performed, we conducted additional work.

Our initial scoping work found that limited SSRs have been performed at the Board. We also found that the Board is transitioning from compliance with the ISM to compliance with requirements promulgated by the NIST, and that NIST does not specifically require these reviews, although having proper software controls in place is discussed in a number of NIST publications. Based on these factors, we closed this project.

In closing the project, however, we provided a report to the Board's CIO in which we recommended that the CIO develop guidance to ensure that single purpose software and other software products are evaluated as part of a general support system, as part of an application security review, or on an individual basis as appropriate. The CIO did not concur with our recommendation and concluded that developing specific guidance for reviewing single purpose software would not be cost-effective. Our recommendation was designed to address not only single purpose software, but also other software products–such as mainframe or telecommunications software–that we believe should be analyzed for potential threats and vulnerabilities, and to help ensure that software does not introduce vulnerabilities or circumvent existing controls. These evaluations can also help set configuration requirements which can then be promulgated throughout the Board. We will continue to review the Board's process for establishing, documenting, and evaluating security controls as part of our ongoing FISMA-related work.

### *Audit of the Board's Fixed Asset Management Process*

During this reporting period, we completed a review of the Board's fixed asset management process. We conducted this audit to evaluate the controls over the receipt, recording, and disposal of fixed assets; determine whether amounts recorded in the Board's general ledger are accurate; identify best practices for conducting, tracking, and recording fixed asset inventories; and evaluate the Board's capitalization policy. As part of our audit, we conducted a physical inventory of a sample of the Board's fixed assets.

Overall, we found that the Board lacks a comprehensive, integrated set of policies, procedures, and internal controls for managing its fixed assets. The current policies governing the Board's fixed asset management process do not

adequately address asset management from a life-cycle perspective and do not include guidance for conducting periodic physical inventories. We believe that a routine physical inventory would have highlighted many of the discrepancies identified during our sample physical inventory. We also found that the Board has not fully implemented features of its financial system which we believe would help establish a more effective property management process. In addition, we identified control weaknesses in the Board's asset disposal process. Through our benchmarking activities, we determined that the Board's capitalization threshold, assets' useful lives, and depreciation method are generally in line with other government and private sector entities.

To address these issues, our report contains two recommendations related to Board policies, financial system usage, and internal controls. Specifically, we recommended that the Director of MGT develop an overall property management policy that governs the receipt, tracking, and disposal of Board assets, to include requirements for conducting periodic physical inventories, and finalize the related accounting policies and procedures. We also recommended that the Director of MGT strengthen internal controls over the Board's property management process by fully implementing available functionality in the Board's financial system, ensuring that sufficient descriptive information is recorded for each asset, and improving controls over the disposal process. We provided a copy of our report to the Director of MGT for review and comment. Her response indicates agreement with the report recommendations and discusses actions that will be taken to implement the recommendations.

### *Investigative Activity*

The OIG is responsible for conducting both criminal and administrative investigations related to alleged fraud, waste, abuse, and employee misconduct. The nature of our workload has evolved over the past years, particularly following the events of September 11, 2001. Since then, the challenges to the federal law enforcement community have generally increased, and our experience and expertise in the financial regulatory environment has been especially in demand. Recently, much of our criminal investigation activity involves leading or participating in multi-agency task forces where bank fraud, terrorist financing, and money laundering are often the potential crimes being investigated.

Our work during this reporting period resulted in criminal charges leading to convictions against two individuals and one administrative action. Fines and restitution resulting from our cases totaled $1,890,679. The following are highlights of our significant investigative activity over the last six months:

- On August 30, 2005, the former president and chief executive officer of Deuel County State Bank was sentenced in the U.S. District Court of Nebraska to forty-eight months incarceration and 120 months supervised

release. The terms of the supervised release prohibit the former president from employment in the banking industry without prior approval from banking regulators. In addition, he was ordered to pay restitution in the amount of $1,888,179. The former president admitted to acts of fraud or defalcation while working in a fiduciary capacity. Specifically, he made loans to himself without Board of Director approval, in amounts which exceeded the bank's limits for loans to insiders, and misstated the purpose for such loans. He waived indictment and entered a plea of guilty to bank fraud. We investigated this case jointly with the FDIC OIG and the Federal Bureau of Investigation (FBI). The case was prosecuted by the U.S. Attorney's Office for the District of Nebraska.

- On June 30, 2005, a South Carolina man was fined $2,500 and sentenced for misuse of fraudulent social security numbers to obtain government documents and establish bank accounts at institutions regulated by the Federal Reserve System. The United States Customs Service is currently in the process of deporting the subject. We investigated this case jointly with the Department of Homeland Security-Coast Guard Investigative Service and the Social Security Administration OIG. The case was prosecuted by the U.S. Attorney's Office for the District of South Carolina.

- We conducted an investigation involving allegations of improper use of a Government Travel Card (GTC) by a Board employee. Our investigation determined that the employee improperly used the GTC to obtain a rental car, non Board-related hotel expenses, a non travel-related cash advance, groceries, and flowers. On May 26, 2005, the OIG issued a Report of Investigation to MGT and the cognizant division director who, as a result of our investigation, took administrative action against the employee.

## Summary Statistics on Investigations for the Period April 1, 2005, through September 30, 2005

| Investigative Actions | Number |
|---|---|
| **Investigative Caseload** | |
| Investigations Opened during Reporting Period | 2 |
| Investigations Open from Previous Period | 11 |
| Investigations Closed during Reporting Period | 5 |
| Total Investigations Active at End of Reporting Period | 8 |
| **Investigative Results for this Period** | |
| Referred to Prosecutor | 0 |
| Joint Investigations | 3 |
| Referred for Audit | 0 |
| Referred for Administrative Action | 1 |
| Oral and/or Written Reprimand | 1 |
| Terminations of Employment | 0 |
| Suspensions | 0 |
| Debarments | 0 |
| Indictments | 0 |
| Convictions | 2 |
| Monetary Recoveries | $0 |
| Civil Actions (Fines and Restitution) | $0 |
| Criminal Fines: Fines & Restitution | $1,890,679 |

## *Hotline Operations*

Our investigators continue to address allegations of wrongdoing related to the Board's programs and operations, as well as violations of the Board's standards of conduct. Most hotline callers were consumers with complaints or questions about practices of private financial institutions. Those inquiries involved matters such as funds availability, account fees and charges, and accuracy and availability of account records. We also continued to receive numerous questions concerning how to process Treasury securities and savings bonds. Other callers contacted us seeking advice about programs and operations of the Board, Federal Reserve Banks, other OIGs, and other financial regulatory agencies. We directed those inquiries to the appropriate Board offices, Reserve Banks, or federal or state agencies. Our summary statistics of the hotline results are provided in the table that follows:

### Summary Statistics on Hotline Results for the Period of April 1,2005, through September 30, 2005

| Complaints Referred for Investigation | Number |
|---|---|
| From the previous reporting period | 17 |
| During this reporting period | 85 |
| **Total for Reporting Period** | 102 |
| | |
| Complaints resolved during this period | 93 |
| Complaints pending | 9 |

## *Executive Council on Integrity and Efficiency Participation*

The Board's IG serves as the Vice Chair of the Executive Council on Integrity and Efficiency (ECIE), which was created by Executive Order in 1992 to facilitate coordination among IGs of designated Federal entities. As Vice Chair, the Board's IG provides leadership, vision, direction, and initiatives for the ECIE on behalf of the Council Chair (OMB's Deputy Director for Management). Collectively, the members of the ECIE have continued to work with the members of the President's Council on Integrity and Efficiency (PCIE) to help improve Government programs and operations.

As ECIE Vice Chair, the Board's IG continues to promote professionalism and coordination among the Councils' membership, provide a forum to discuss government-wide issues and shared concerns, and facilitate work on a wide range of Council projects and initiatives. *A Progress Report to the President, Fiscal Year 2004,* an annual publication that is available on the IG community's website at www.ignet.gov, highlights the collective work and accomplishments of the IG community and the Councils' progress toward achieving strategic goals and objectives.

## *OIG Peer Review*

*Government Auditing Standards* require organizations performing audits in accordance with these standards to undergo an external peer review of their auditing practices at least once every three years. During this reporting period, staff from the Pension Benefit Guaranty Corporation (PBGC) OIG reviewed our audit operations. The review's overall objective was to obtain reasonable assurance that the Board's OIG followed established policies and procedures and applicable auditing standards in performing audit work.

In the opinion of the PBGC OIG, the system of quality control for the audit function of the Board's OIG has been designed in accordance with the quality standards established by the PCIE and was being complied with for the year ended March 31, 2005, to provide the OIG with reasonable assurance of material compliance with professional auditing standards in the conduct of its audits. The PBGC OIG therefore issued an unqualified opinion on our system of audit quality control. We provided a copy of the peer review report to each member of the Board.

## *Review of Legislation and Regulations*

Pursuant to the IG Act, as amended, we review existing and proposed legislative and regulatory items both as part of our routine activities and on an ad hoc basis. We routinely track proposed and pending legislation and regulations and are also requested to provide comments on revisions or additions to Board management policy statements. We then independently analyze the effect that the new or proposed legislation, regulation or policy may have on the efficiency and effectiveness of the programs and operations of the Board, including the OIG. During the current reporting period, we reviewed twenty-four legislative items and two Board management policy statements. The following table highlights our work in this area during the current reporting period.

## Highlights of the OIG's Review of Laws and Regulations, April 1, 2005, through September 30, 2005

| Legislation Reviewed | Purpose/Highlights |
|---|---|
| **Board-related Legislation** | |
| Business Checking Freedom Act of 2005 (H.R. 1224) | To amend the Federal Reserve Act and, among other things, repeal the prohibition on depository institution payment of interest on business checking accounts. |
| Due Process and Economic Competitive Restoration Act (H.R. 1657); Competitive Enhancement and Opportunity Act of 2005 (H.R. 1641) | To lessen any adverse economic impact associated with section 404 of the Sarbanes-Oxley Act of 2002. |
| **IG Community** | |
| Improving Government Accountability Act (H.R. 2489) | To amend the IG Act to enhance the operations of the IG community. Introduced on May 19, 2005. Ongoing coordination with Congressional staff and PCIE/ECIE legislation committee regarding the bill's requirements. |
| Section 522 of the Consolidated Appropriations Act of 2005 | Requires the appointment of a chief privacy officer; establishes requirements for handling privacy information and audit responsibilities of certain IGs. |
| Inspector General Online Reporting Act | Requires all OIG reports to be made available online. Our comments, along with those of other IG offices, have led to delay of bill's introduction pending revisions. |
| Hurricane Katrina Related: H.R. 3805, H.R. 3810, H.R. 3737, and S. 1738 | Proposals for IG oversight related to expenditures of Hurricane Katrina disaster relief funds |
| **Employee-related and Information-related Legislation** | |
| HELPS Retirees Act of 2005 (H.R. 2177) and related bills H.R. 994, S. 484 | Allows tax relief for certain categories of federal/military employees. |
| Faster FOIA Act of 2005 (H.R. 1620) | To speed up the Freedom of Information Act (FOIA) process by changing procedures. |
| S. 1181 | A bill to ensure an open and deliberate process in Congress by providing that any future legislation establishing a new exemption to the FOIA must explicitly state such exemption within the text of the legislation. |

# Follow-Up Activities

Over the past six months, we have conducted follow-up work on the open recommendations related to three prior OIG reports. The status of our follow-up work is summarized below, including the recommendations that we have closed and those recommendations where follow-up review work is still in process.

### *Audit of the Board's Security-Related Directed Procurements*

We completed follow-up work related to our September 2002 *Report on the Audit of the Board's Security-Related Directed Procurements*. Our report contained two recommendations designed to strengthen the policies and procedures over unique purchases and a third recommendation related to strengthening controls over payments related to fixed-unit-price service contracts. Prior follow-up work allowed us to close our recommendations related to policies and procedures.

Regarding our third recommendation, MGT instituted mandatory training for all Contracting Officer's Technical Representatives (COTRs) and provided written guidance during the training which requires COTRs to confirm contractor deliveries or performance and to verify documentation supporting vendor invoices such as the number of hours and hourly rates. Based on the guidance and training provided, we have closed the final recommendation.

### *Audit of the Federal Reserve Board's Government Travel Card Program*

Our January 2002 report contained five recommendations designed to help the Board establish and communicate clear guidance on the travel card program and to improve internal controls over issuing, monitoring, and canceling GTCs. We previously closed our recommendations related to providing additional guidance regarding employee use of the GTC and developing internal operating procedures for GTC processes. During this reporting period, we reviewed revised procedures related to controls over the authorization process, monitoring employee credit card use, and closing accounts. We found that MGT now performs bi-weekly reviews of GTC transactions to help monitor credit limits and intends to provide cards to new employees only when they have a requirement for the card in order to travel or attend training. MGT staff also developed procedures for handling violations of the Board's travel regulations regarding GTC use and improved the retention of documentation regarding actions taken when violations are detected. Finally, we tested a list of active cardholders against a list of current employees in the Board's personnel system and found that MGT staff improved controls over closing GTC accounts by developing procedures to timely deactivate cards and close departing employee accounts. The actions taken are sufficient for us to close our remaining recommendations.

### *Audit of Retirement Plan Administration*

Our July 2003 audit report contained four recommendations describing policy decisions that the Board, either through the Committee on Board Affairs (CBA) or through its representation on other Systemwide oversight committees, needed to make to strengthen oversight and administration of the retirement plan. Last year, we closed our recommendation regarding the methodology for allocating benefit-related expenses to the Board and Reserve Banks and, in the first quarter of this year, closed our recommendation that the CBA establish clear guidance for the role of MGT staff in support of retirement processing. Since then, we have conducted additional follow-up work, including interviews with responsible Board staff and reviews of revised processes and related documentation.

To address our recommendation regarding the establishment of an audit committee, Board staff discussed this issue with Board and System officials (including several of the Governors) who seemed satisfied with the current level of oversight. None of these officials favored the creation of another oversight committee. Nevertheless, the Committee on Plan Administration (CPA), which has primary oversight responsibility for the audit function of the Office of Employee Benefits (OEB) and the retirement plan and assets, has made a commitment to provide greater coordination of audit matters with the other retirement plan committees. We reviewed the revised CPA charter and found that the CPA's responsibilities include sharing external audit reports and management letters with the other committees, as well as with the System's Conference of Presidents and the Conference of General Auditors. We believe these actions are sufficient to close this recommendation.

Regarding our final recommendation, we found that the outsourced contractor has revised its methodology for including lump sum payments in the retirement calculation and that Board staff are working with OEB to revise the Retirement Plan documents to reflect this change. We tested a judgmental sample of ten recent retirees to verify the processing changes and found that the calculations were incorrect for two of the retirees in our sample. Although the discrepancies were minor and immediate action was taken to correct the errors, we plan to perform additional testing during the coming months before closing this recommendation.

# Appendixes

## Appendix 1

## Audit Reports Issued with Questioned Costs for the Period April 1, 2005, through September 30, 2005

| Reports | Number | Dollar Value | |
|---|---|---|---|
| | | Questioned Costs | Unsupported |
| For which no management decision had been made by the commencement of the reporting period | 0 | $0 | $0 |
| That were issued during the reporting period | 0 | $0 | $0 |
| For which a management decision was made during the reporting period | 0 | $0 | $0 |
| (i) dollar value of disallowed costs | 0 | $0 | $0 |
| (ii) dollar value of costs not disallowed | 0 | $0 | $0 |
| For which no management decision had been made by the end of the reporting period | 0 | $0 | $0 |
| For which no management decision was made within six months of issuance | 0 | $0 | $0 |

## Appendix 2

## Audit Reports Issued with Recommendations that Funds be Put to Better Use for the Period April 1, 2005, through September 30, 2005

| Reports | Number | Dollar Value |
|---|---|---|
| For which no management decision had been made by the commencement of the reporting period | 0 | $0 |
| That were issued during the reporting period | 0 | $0 |
| For which a management decision was made during the reporting period | 0 | $0 |
| (i) dollar value of recommendations that were agreed to by management | 0 | $0 |
| (ii) dollar value of recommendations that were not agreed to by management | 0 | $0 |
| For which no management decision had been made by the end of the reporting period | 0 | $0 |
| For which no management decision was made within six months of issuance | 0 | $0 |

# Appendix 3
# OIG Reports with Outstanding Recommendations

| Projects Currently Being Tracked | Issue Date | Recommendations | | | Status of Recommendations[1] | | |
|---|---|---|---|---|---|---|---|
| | | No. | Mgmt. Agrees | Mgmt. Disagrees | Follow-up Completion Date | Closed | Open |
| Business Process Review of the Board's Travel Administration | 07/97 | 9 | 9 | 0 | 11/04 | 6 | 3 |
| Audit of the Board's Efforts to Implement Performance Management Principles Consistent with the Results Act | 07/01 | 4 | 4 | 0 | 08/03 | 0 | 4 |
| Audit of the Federal Reserve's Background Investigation Process | 10/01 | 3 | 3 | 0 | 04/04 | 0 | 3 |
| Audit of the Federal Reserve Board's Government Travel Card Program | 01/02 | 5 | 5 | 0 | 09/05 | 5 | 0 |
| Audit of the Board's Security-Related Directed Procurements | 09/02 | 3 | 2 | 1 | 06/05 | 3 | 0 |
| Audit of Retirement Plan Administration | 07/03 | 4 | 3 | 1 | 06/05 | 3 | 1 |
| Audit of the Board's Outsourcing Operations | 04/04 | 3 | 3 | 0 | – | – | – |
| Review of the Fine Arts Program | 04/04 | 2 | 2 | 0 | – | – | – |
| Effectiveness of Administrative Controls Over an Outsourced Contract | 06/04 | 2 | 2 | 0 | – | – | – |
| Audit of the Board's Information Security Program | 09/04 | 5 | 5 | 0 | 09/05 | 2 | 3 |
| Audit of the Board's Automated Travel System | 11/04 | 4 | 4 | 0 | 02/05 | 1 | 3 |
| Review of the Board's Workers' Compensation Program | 03/05 | 4 | 4 | 0 | – | – | – |
| Review of the Board's Implementation of Software Security Reviews | 05/05 | 1 | 0 | 1 | – | – | – |
| Audit of the Board's Fixed Asset Management Process | 05/05 | 2 | 2 | 0 | – | – | – |
| Evaluation of Service Credit Computations | 08/05 | 3 | 3 | 0 | – | – | – |
| Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act | 09/05 | 4 | 3 | 1 | – | – | – |
| Audit of the Board's Information Security Program | 10/05[2] | 2 | 2 | 0 | – | – | – |

[1] A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable, or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the Board is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred it to the appropriate oversight committee or administrator for a final decision.

[2] Since our FISMA work was completed during this semiannual reporting period, we have included it in this semiannual report. The final FISMA report was formally issued on October 6, 2005.

## Appendix 4

## Cross-References to the Inspector General Act

## Indexed below are the reporting requirements prescribed by the Inspector General Act of 1978, as amended, for the reporting period:

| Section | Source | Page(s) |
|---|---|---|
| 4(a)(2) | Review of legislation and regulations | 14 |
| 5(a)(1) | Significant problems, abuses, and deficiencies | None |
| 5(a)(2) | Recommendations with respect to significant problems | None |
| 5(a)(3) | Significant recommendations described in previous Semiannual Reports on which corrective action has not been completed | None |
| 5(a)(4) | Matters referred to prosecutory authorities | 12 |
| 5(a)(5) | Summary of instances where information was refused | None |
| 5(a)(6) | List of audit reports | 4-10 |
| 5(a)(7) | Summary of significant reports | None |
| 5(a)(8) | Statistical Table—Questioned Costs | 21 |
| 5(a)(9) | Statistical Table—Recommendations that Funds Be Put to Better Use | 22 |
| 5(a)(10) | Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made | 23 |
| 5(a)(11) | Significant revised management decisions made during the reporting period | None |
| 5(a)(12) | Significant management decisions with which the Inspector General is in disagreement | None |

*Inspector General Hotline*
*1-202-452-6400*
*1-800-827-3340*

*Report: Fraud, Waste or Mismanagement*
*Information is confidential*
*Caller can remain anonymous*

*You may also write the:*
*Office of Inspector General*
*HOTLINE*
*Mail Stop 300*
*Board of Governors of the Federal Reserve System*
*Washington, DC 20551*